

IN THE UNITED STATES DISTRICT COURT  
FOR THE SOUTHERN DISTRICT OF OHIO  
WESTERN DIVISION

|                                 |   |                               |
|---------------------------------|---|-------------------------------|
| Steven Warshak, <i>et al.</i> , | : | Case No. 1:06-cv-357          |
|                                 | : |                               |
| Plaintiffs,                     | : | District Judge Susan J. Dlott |
|                                 | : |                               |
| v.                              | : | ORDER GRANTING IN PART AND    |
|                                 | : | DENYING IN PART PLAINTIFF     |
| United States,                  | : | STEVEN WARSHAK’S MOTION FOR   |
|                                 | : | TRO AND/OR PRELIMINARY        |
| Defendant.                      | : | INJUNCTION AND ENTERING       |
|                                 | : | PRELIMINARY INJUNCTION        |

This matter comes before the Court on the Motion of Plaintiff Steven Warshak (“Warshak”)<sup>1</sup> for Issuance of a Temporary Restraining Order (TRO) and/or Preliminary Injunction (“Motion”). (Doc. #11.) For the reasons below, the Court **GRANTS IN PART AND DENIES IN PART** Warshak’s Motion and **PRELIMINARILY ENJOINS** the United States from seizing, pursuant to court order issued under 18 U.S.C. § 2703(d), the contents of any personal email account maintained by an Internet Service Provider (“ISP”) in the name of any resident of the Southern District of Ohio without providing the relevant account holder or subscriber prior notice and an opportunity to be heard.

## **I. BACKGROUND**

Warshak filed this lawsuit in June 2006, alleging that the United States violated both the Fourth Amendment to the United States Constitution and certain provisions of the Stored Communications Act (“SCA”), 18 U.S.C. § 2701 et seq., by directing two ISPs to produce

---

<sup>1</sup> “Warshak,” in this Order, refers only to original plaintiff Steven Warshak and not to Intervenor-Plaintiff Harriet Warshak. (Doc. #20.)

certain electronic mail (“email”) of Warshak’s from their servers pursuant to warrantless search orders issued under the authority of SCA Section 2703(d) (“2703(d) orders”). (Doc. #1-1 at 1-2.) In his present Motion (doc. #11), Warshak seeks to prospectively enjoin the United States from obtaining and enforcing any future 2703(d) orders.

**A. Factual Background**

In March 2005, the United States was engaged in a criminal investigation into allegations of mail and wire fraud, money laundering, and other federal offenses in connection with the operations of Berkeley Premium Nutraceuticals, Inc. (“Berkeley”) a company owned by Warshak. (See, e.g., doc. #1 Ex. 1 at 1.) On May 6, 2005, the United States obtained an order from a United States Magistrate Judge for the Southern District of Ohio directing NuVox Communications, an ISP, to turn over to inspectors or agents of the United States Postal Service and Federal Bureau of Investigation “within three (3) days” “all customer account information for any accounts registered or services rendered to” Warshak or “associated parties,” including<sup>2</sup>

The contents of wire or electronic communications (not in electronic storage unless greater than 181 days old) that were placed or entered in directories or files owned or controlled by [Warshak’s accounts] at any time during the hosting of the electronic communications and through the date of this Order . . . .  
Communications not in “electronic storage” include any e-mail communications received by the specified accounts that the owner or user of the accounts has already accessed, viewed, or downloaded.

(Id. at 3.)

The Magistrate Judge noted that the order was issued pursuant to 18 U.S.C. § 2703(d), a

---

<sup>2</sup> The order also directed NuVox to turn over “all log files and backup tapes”; customer “account identifiers”; “application information”; “contact information”; “email addresses”; “billing information to include bank account numbers”; and “any other information pertaining to the customer, including setup, synchronzation.” (Doc. #1 Ex. 1 at 3.)

subsection of the SCA, and upon a finding that the United States had “offered specific and articulable facts showing that there are reasonable grounds to believe that the records or other information sought are relevant and material to an ongoing criminal investigation.” (Id. at 2.) The Magistrate Judge also found that “prior notice of this Order to any person of this investigation of this application and order by the government or NuVox would seriously jeopardize the investigation.” (Id.) Accordingly, he ordered the application and order sealed “until otherwise ordered by the Court” and provided that “the notification by the government otherwise required under [SCA subsection] 18 U.S.C. § 2703(b)(1)(B) be delayed for ninety days.” (Id.)

On September 12, 2005, the United States obtained a second and virtually identical<sup>3</sup> ex parte 2703(d) order against two email accounts apparently maintained for Warshak by Yahoo communications, another ISP. (Doc. #1 Ex. 2.)

On May 31, 2006, over a year after obtaining the NuVox 2703(d) order and nine months after obtaining the Yahoo 2703(d) order, the United States wrote to Warshak to notify him of the orders.<sup>4</sup> (Doc. #1 Ex. 1 at 1, Ex. 2 at 1.) The Magistrate Judge had unsealed both orders the previous day, May 30, 2006, apparently on the United States’ motion. (See 1:05-mj-135, docs. ##s 3-4 and 1:05-mj-216, docs. ##s 3-4.)

## **B. Procedural Background**

---

<sup>3</sup> The Yahoo 2703(d) order sought information for an account maintained in the name of “Ron Fricke,” but – unlike the NuVox order – did not broadly request information for any unidentified parties “associated” with Warshak. (Doc. #1 Ex. 2 at 3; cf. doc. #1 Ex. 1 at 3.)

<sup>4</sup> The United States attached copies of the orders to its notice letters. (Doc. #1 Ex. 1 at 1, Ex. 2 at 1.)

Warshak filed his Fourth Amendment and SCA complaint against the United States on June 12, 2006, approximately two weeks after receiving formal notice of the NuVox and Yahoo 2703(d) orders and seizures. (Doc. #1.) On July 1, 2006, Warshak filed his instant Motion to enjoin the United States from “further implementation and/or use of the SCA to access any [of Warshak’s] email communications unless pursuant to a search warrant lawfully issued upon a showing of probable cause, pursuant to the first sentence of 18 U.S.C. § 2703(a), or pursuant to 18 U.S.C. § 2510.” (Doc. #11; doc. #1-1 at 15 ¶ 3.)<sup>5</sup> The Court held a telephonic hearing with the parties<sup>6</sup> on July 5, 2006, after which it took the matter under submission. (Docs. ##s 12, 15.) The Motion is now fully briefed and ripe for review. (Docs. ##s 11, 15, 16, 17.)<sup>7</sup>

## II. ANALYSIS

In determining whether to issue a preliminary injunction, the Court must consider (1) whether Warshak has shown a strong or substantial likelihood of success on the merits of his claims against the United States; (2) whether Warshak has shown that irreparable injury will result if no injunction issues; (3) whether the issuance of a preliminary injunction would substantially harm the United States or others; and (4) whether the issuance of a preliminary

---

<sup>5</sup> Warshak’s Motion and Memorandum in support of a TRO and/or preliminary injunction describes the relief sought by reference to Warshak’s complaint. (See doc. #11 at 2-3 ¶¶ 4-5.) Warshak’s complaint seeks other injunctive relief not described above, as well as declaratory relief. (See doc. #1-1 at 14-15 ¶¶ 1-2, 4-5.) Warshak’s counsel confirmed at the telephonic motion hearing that his present Motion concerns only the above-referenced relief.

<sup>6</sup> At the time of the telephonic hearing, Steven Warshak was the sole plaintiff. However, the Court allowed counsel for Harriet Warshak and Paul Kellogg, both of whom had moved to intervene and have since been joined as plaintiffs, to participate. (Docs. ##s 13, 14, 20.)

<sup>7</sup> Warshak filed two separate reply memoranda. (Docs. ##s 16, 17.) Because the filings are both timely and jointly comprise only seven pages, and because the United States has not objected to the dual submission, the Court has exercised its discretion to consider both memoranda in deciding Warshak’s Motion.

injunction would serve the public interest. Deja Vu of Nashville, Inc., v. Metro. Gov't of Nashville & Davidson C'ty, 274 F.3d 377, 400 (6<sup>th</sup> Cir. 2001). For the reasons below, the Court finds that while the broad preliminary injunction sought by Warshak is unwarranted, narrower relief is appropriate to ensure that Warshak's constitutional rights are not infringed pending a final decision on the merits of Plaintiffs' claims.

**A. Preliminary Injunction Factors**

**1. Likelihood of Success on the Merits**

Warshak contends that the United States must be enjoined from seeking further 2703(d) email seizure orders because such orders, to the extent they are "premised upon a showing of less than probable cause, clearly do not constitute a judicially issued search warrant" and thus violate the Fourth Amendment.<sup>8</sup> (Doc. #11 at 7-8.) Warshak further asserts that he is also entitled to an injunction because future 2703(d) orders of the type the United States used to seize his NuVox and Yahoo emails would be unlawful under the terms of the SCA itself. (Id. at 14.)

**a. Fourth Amendment Claim**

Section 2703 of the SCA provides, in relevant part:

**(a) Contents of wire or electronic communications in electronic storage.** – A governmental entity may require the disclosure by a provider of electronic communication service of the contents of a wire or electronic communication, that is in electronic storage in an electronic communications system for one hundred and eighty days or less, only pursuant to a warrant issued using the procedures described in the Federal Rules of Criminal Procedure by a court with jurisdiction over the offense under investigation or equivalent State warrant. A governmental entity may require the disclosure by a provider of electronic communications services of the contents of a wire or electronic communication that has been in electronic storage in an electronic communications system for more than one hundred and eighty days by the means available under subsection (b) of this section.

---

<sup>8</sup> Warshak further contends that for this same reason, 2703(d) orders violate Federal Rule of Criminal Procedure 41. (Id.) Rule 41 clearly states, however, that it "does not modify any statute regulating search or seizure. . . ." Fed. R. Crim. P. 41(a)(1). The more relevant substantive inquiry, therefore, is whether Section 2703(d) of the SCA – a federal statute regulating search and seizure of wire and electronic communications – violates the search and seizure protections of the Fourth Amendment itself.

**(b) Contents of wire or electronic communications in a remote computing service. –**

(1) A governmental entity may require a provider of remote computing service to disclose the contents of any wire or electronic communication to which this paragraph is made applicable by paragraph (2) of this subsection –

(A) without required notice to the subscriber or customer, if the governmental entity obtains a warrant issued using the procedures described in the Federal Rules of Criminal Procedure by a court with jurisdiction over the offense under investigation or equivalent State warrant; or

(B) with prior notice from the governmental entity to the subscriber or customer if the governmental entity –

[\* \* \* \*]

(ii) obtains a court order for such disclosure under subsection (d) of this section; except that delayed notice may be given pursuant to section 2075. . . .<sup>9</sup>

---

<sup>9</sup> 18 U.S.C. § 2075 provides, in relevant part:

**(a) Delay of notification. –**

(1) A governmental entity acting under section 2703(b) of this title may –

(A) where a court order is sought, include in the application a request, which the court shall grant, for an order delaying the notification required under section 2703(b) of this title for a period not to exceed ninety days, if the court determines that there is reason to believe that notification of the existence of the court order may have an adverse result described in paragraph (2) of this subsection . . . .

(2) An adverse result for the purposes of paragraph (1) of this subsection is –

(A) endangering the life or physical safety of an individual;

(B) flight from prosecution;

(C) destruction of or tampering with evidence;

(D) intimidation of potential witnesses; or

(E) otherwise seriously jeopardizing an investigation or unduly delaying a trial.

[\* \* \* \*]

(4) Extensions of the delay of notification provided in section 2703 of up to ninety days each may be granted by the court upon application, or by certification by a governmental entity, but only in accordance with subsection (b) of this section.

(5) Upon expiration of the period of delay of notification under paragraph (1) or (4) of this subsection, the governmental entity shall serve upon, or deliver by registered or first-class mail to, the customer or subscriber a copy of the process or request together with notice that –

(A) states with reasonable specificity the nature of the law enforcement inquiry; and

(B) informs such customer or subscriber –

(i) that information maintained for such customer or subscriber by the service provider named in such process or request was supplied to or requested by that governmental authority and the date on which the supplying or request took place;

(ii) that notification of such customer or subscriber was delayed;

(iii) what governmental entity or court made the certification or determination pursuant to which that delay was made; and

(iv) which provision of this chapter allowed such delay.

[\* \* \* \*]

[\* \* \* \*]

**(d) Requirements for court order.** – A court order for disclosure under subsection (b) or (c) may be issued by any court that is a court of competent jurisdiction and shall issue only if the governmental entity offers specific and articulable facts showing that there are reasonable grounds to believe that the contents of a wire or electronic communication, or the records or other information sought, are relevant and material to an ongoing criminal investigation. . . .

18 U.S.C. § 2703 (emphasis added).

The Fourth Amendment provides that

The right of people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the person or things to be seized.

U.S. Const. amend. IV.

The parties agree that the standard of proof outlined in 18 U.S.C. § 2703(d) – “specific and articulable facts showing that there are reasonable grounds to believe that the contents” of the email account to be seized “are relevant and material to an ongoing criminal investigation” – falls somewhere short of probable cause. (See, e.g., doc. #15 at 4 (United States’ opposition).)

Warshak asserts that in relying on this lesser standard to seize his emails, the United States violated the longstanding Fourth Amendment presumption that “closed packages and containers

---

**(b) Preclusion of notice to subject of governmental access.**– A governmental entity acting under section 2703, when it is not required to notify the subscriber or customer under section 2703(b)(1), or to the extent that it may delay such notice pursuant to subsection (a) of this section, may apply to a court for an order commanding a provider of electronic communications service or remote computing service to whom a warrant, subpoena, or court order is directed, for such period as the court deems appropriate, not to notify any other person of the existence of the warrant, subpoena, or court order. The court shall enter such an order if it determines that there is reason to believe that notification of the existence of the warrant, subpoena, or court order will result in –

- (1) endangering the life or physical safety of an individual;
- (2) flight from prosecution;
- (3) destruction of or tampering with evidence;
- (4) intimidation of potential witnesses; or
- (5) otherwise seriously jeopardizing an investigation or unduly delaying a trial.

may not be searched without a warrant” issued upon a showing of probable cause. United States v. Ross, 456 U.S. 798, 811-812 and n. 16 (1982). He analogizes emails stored in personal accounts on the servers of commercial ISPs to the contents of “[l]etters and other sealed packages” shipped by public or private carriers, a class of effects for which warrantless searches are “presumptively unreasonable.” (Doc. #11 at 8 (citing in part United States v. Jacobsen, 466 U.S. 109, 114 (1982).) While “government agents may lawfully *seize*” such effects “to prevent loss or destruction of suspected contraband, the Fourth Amendment requires that [government agents] obtain a warrant before examining the *contents*” of letters or packages. Jacobsen, 466 U.S. at 114 (emphasis added); see also Ross, 456 U.S. 812 n. 16 (noting that there is “significant difference between the seizure of a sealed package and a subsequent search of its contents,” with the latter constituting a “far greater intrusion into Fourth Amendment values . . . .”)

The United States argues that a personal email held by a commercial ISP resembles less a sealed letter than a postcard amenable to warrantless inspection, because “its contents are plainly visible to the [ISP], who can access it via its servers at any time.” (Doc. #15 at 10; see also United States v. Van Leeuwen, 397 U.S. 249, 251 (1970) (distinguishing letters and sealed packages from newspapers, circulars and similar printed matter sent through the mail).) It asserts that ISPs typically reserve the right to access, delete, or turn over to law enforcement personal emails stored on their servers and routinely do access such emails at least to the extent necessary to screen for viruses, spam, and illegal pornographic materials. (Doc. #15 at 10-12.) As such, the United States contends that the more apt Fourth Amendment analogy is to personal information already opened by or otherwise made visible to non-governmental third parties, which may generally be seized with subpoenas issued on less than a showing of probable cause.



(Doc. #15 at 8-12 (citing in part United States v. Miller, 425 U.S. 435 (1976), and Couch v. United States, 409 U.S. 322, 335 (1973).) It submits – and Warshak does not appear to dispute – that the “specific and articulable” facts standard articulated in 2703(d) is at least as stringent as the standard of proof applied to subpoenas. (See, e.g., doc. #15 at 4 (citing H. Rep. No. 103-827(I), at 31 (1996), reprinted in 1996 U.S.C.C.A.N. 3489, 3511 (legislative description of 2703(d) standard as “higher than a subpoena, but not a probable cause warrant.”)).)

The Supreme Court has held that “when an individual *reveals* private information to another, he assumes the risk that the confidant will reveal that information to the authorities, and if that occurs the Fourth Amendment does not prohibit governmental use of that information.” Jacobsen, 466 U.S. at 118 (emphasis added). That is because an individual cannot maintain any “reasonable expectation of privacy” – the test for standing to challenge a warrantless seizure under the Fourth Amendment – in once-private information he has already effectively shared with a third party. (Id.) The question, therefore, is whether it is reasonable to assume that once personal emails are stored on a commercial ISP’s server, whatever expectation of privacy the account subscriber may have had in those emails has “already been frustrated.” (Id.) The limited record presently before the Court suggests that it is not.

While emails sent through and stored on the servers of commercial ISPs are obviously distinguishable in many respects from both sealed letters and postcards physically mailed via public or private carrier, the letter analogy appears – on the limited evidence presently before the Court – to be more apt. As Warshak persuasively argues:

[I]n the case of email, the subscriber perhaps maintains *more* control over the email letter than in any other traditional third party carrier context. In the latter scenarios, the sender or receiver of a closed letter or package actually relinquishes control of the container and cannot immediately repossess the letter or package – it is in the physical possession of the postal carrier and/or common carrier outside the dominion and control of the sender or recipient. In the email context, the owner of the email can repossess a read-and-then-closed email at any moment, without any notice or permission from the ISP, can retake the email, delete the email from his mailbox, or do what she wants to do with the email . . . .

(Doc. #11 at 10 (emphasis added).) The United States has asserted in its papers and at oral argument that the privacy expectations attributed to letters entrusted to third-party carriers are inapposite to emails entrusted to commercial ISPs, because ISPs and individual account holders routinely both reserve and exercise rights to open, delete, or turn over personal emails to law enforcement. As the parties noted at oral argument, however, the terms of service governing email accounts can vary from ISP to ISP. At oral argument, Warshak also challenged the United States’ assertion that ISPs routinely “access” the emails in their subscribers’ individual accounts in any meaningful Fourth Amendment sense. Although Warshak did not appear to contest the United States’ more specific assertion that ISPs can and do screen emails for objectively damaging or illegal content such as viruses or child pornography,<sup>10</sup> he strenuously disputed the presumption that employees of commercial ISPs open and read – or their subscribers reasonably

---

<sup>10</sup> This screening for illegal content, even assuming it happens as a matter of course, does not appear to the Court to destroy the analogy between the contents of email accounts and the contents of sealed packages or letters. The Supreme Court has held that once agents for a private carrier have opened and viewed the contents of a suspicious package without any government prompting, the government may reexamine those exposed contents without violating the Fourth Amendment’s warrant requirements. Jacobsen, 466 U.S. at 115-116. However, it has also rejected the proposition that government authorities may rely on broad private searches to circumvent their Fourth Amendment obligations. See, e.g., Jacobsen, 466 U.S. at 117-18. By analogy, it would seem that even if an ISP’s discovery that a subscriber email contained child pornographic content gave the government sufficient grounds to seize and view that email without a warrant, it would not necessarily follow that the government could routinely seize and view the contents of entire email accounts not known to contain any illegal material.

expect them to open and read – individual subscriber emails as a matter of course.

While the Court is prepared to reconsider its views upon the presentation of further evidence on these points, it is not persuaded – as an initial matter – that an individual surrenders his reasonable expectation of privacy in his personal emails once he allows those emails (or electronic copies thereof) to be stored on a subscriber account maintained on the server of a commercial ISP.<sup>11</sup> As such, the Court finds that Warshak has shown a substantial likelihood of success on the merits of his Fourth Amendment claim. The first factor of the preliminary injunction test thus weighs in favor of relief. Deja Vu, 274 F.3d at 400.

**b. Stored Communications Act (SCA) Claim**

Because Warshak has demonstrated a sufficient likelihood of success on his Fourth Amendment claim to support an injunction under the first factor of the test for preliminary injunctive relief, the Court need not reach, for purposes of the present Motion, the merits of Warshak's secondary claim that the 2703(d) orders obtained and/or threatened by the United States in this matter violate the SCA. Instead, the Court proceeds to consider whether the remaining factors of the preliminary injunction test also weigh in favor of relief.

**2. Irreparable Injury to Warshak**

The Court next considers whether, under the second factor of the preliminary injunction test, Warshak will suffer “irreparable harm” if his Motion is denied. Deja Vu, 274 F.3d at 400.

---

<sup>11</sup> In so holding, the Court does not distinguish between messages read and unread by the subscriber, between messages newer or older than 180 days, or between originals and backup electronic copies. The parties have focused on such distinctions primarily in the context of Warshak's secondary claim that the United States has misapplied the SCA, the merits of which the Court does not reach today. See Part II.A.1.b, infra. They may also prove relevant in the Court's ultimate disposition of Warshak's constitutional claim, but the Court cannot so conclude on the present, limited record.

A finding of “irreparable harm” ordinarily flows automatically from a court’s finding, under the first factor of the test, that a constitutional right is being threatened or impaired. American Civil Liberties Union of Kentucky v. McCreary County, Kentucky, 354 F.3d 438, 445 (6<sup>th</sup> Cir. 2003) (citing Elrod v. Burns, 427 U.S. 347, 373 (1976)). Nonetheless, for the sake of completeness, the Court will briefly address the specific arguments raised by the parties.

**i. “Imminent” or “Speculative” Harm**

The United States first asserts, by reference to the Sixth Circuit’s decision in Abney v. Amgen, Inc., 443 F.3d 540, 552 (6<sup>th</sup> Cir. 2006), that Warshak cannot satisfy this standard because he cannot show that he would necessarily suffer any “actual or imminent” harm, as opposed to merely “speculative or unsubstantiated” harm, if no injunction were to issue. (Doc. #15 at 17.) Warshak responds that in light of the “ex parte process . . . repeatedly employed by the United States” in prior seizures of his email from ISPs, he cannot fairly be penalized for his “[in]ability to identify” any precise future moment at which the United States might next obtain and enforce a 2703(d) seizure order against him. (Doc. #16 at 1.)

Warshak’s contentions are well-taken. It is undisputed that the United States has already conducted two warrantless, ex parte 2703(d) seizures of email accounts maintained for Warshak by commercial ISPs. Moreover, at least as of the July 5, 2006 telephonic hearing on Warshak’s Motion, the United States has refused to pledge not to obtain or enforce future 2703(d) orders of this kind against other email accounts of Warshak’s. While these facts are obviously not conclusive proof that the United States will seek future *ex parte* 2703(d) orders, the Court is satisfied that the prospective harm in this case is far from “speculative” or “unsubstantiated”

under Amgen.<sup>12</sup> Indeed, to the extent that the merit of Warshak's claims that the contemplated seizures are unconstitutional ultimately turns on the seizures' *ex parte* nature, it would be ironic for the Court to refuse to prospectively enjoin those seizures on the grounds that Warshak cannot predict exactly when or whether they may occur. See also discussion at Part II.B., infra.

## ii. Adequate Alternative Remedies at Law

The United States also asserts that Warshak will not suffer irreparable injury if an injunction does not issue because the SCA, by its own terms, provides him adequate protection against arbitrary seizures of his email. (Doc. #15 at 18.) It first observes that under the plain terms of the statute, no 2703(d) order may issue until the United States presents, and a judicial officer finds, "specific and articulable facts showing that there are reasonable grounds to believe" that the targeted emails "are relevant and material to an ongoing criminal investigation." (Id. (citing 18 U.S.C. 2703(d).) This observation, however, simply begs the constitutional question: 2703(d)'s existing safeguards are legally adequate only to the extent they pass muster under the Fourth Amendment, and the Court has just found a substantial likelihood that they do not. See Part II.A.1, infra. The United States further notes that even if it were to seek further 2703(d) orders against Warshak, "it would be required to provide Warshak prior notice unless it could satisfy the delayed notice provisions of § 2705(a)," and Warshak has not shown "any

---

<sup>12</sup> In Amgen, participants in a clinical drug trial of a new treatment for Parkinson's disease terminated by the manufacturer sought a preliminary injunction that would have forced the manufacturer to continue providing them with the drugs used in the trial. Amgen, 443 F.3d at 542. In affirming the district court's denial of that injunction, the Sixth Circuit noted that while there was "no question that plaintiffs' health [would] continue to deteriorate as a result of their Parkinson's disease," there was a significant evidentiary conflict as to whether the requested treatment would arrest or delay that deterioration. Id. at 552. Here, there is no apparent dispute that the requested injunction, if granted, would avert the prospective harm Warshak describes.

reason to believe” the United States could satisfy those provisions. (Doc. #15 at 19.) The fact the United States has already twice obtained the protection of 2705(a), however, would appear to be reason enough.<sup>13</sup> Finally, the United States notes that if Warshak can ultimately show, on the merits, that the United States has “willfully violated his rights *under* the SCA,” the statute affords him a cause of action for money damages. (*Id.* (emphasis added) (citing 18 U.S.C. § 2712).) It does not necessarily follow, however, that money damages would adequately remedy any unconstitutional *application* of the SCA to Warshak.<sup>14</sup> See, e.g., McCreary County, Kentucky, 354 F.3d at 445 (threatened constitutional injury presumptively “irreparable” under four-factor test for preliminary injunctive relief).

For all these reasons, the second factor of the analysis also weighs in favor of relief.

### **3. Governmental and Public Interests**

Before granting preliminary injunctive relief to Warshak, the Court must also consider (3) whether the issuance of an injunction would substantially harm the United States or other

---

<sup>13</sup> The United States’ assertion that 2705(a) affords Warshak adequate legal protection is further belied by the suggestion, in the current record, that the United States did not strictly adhere to the requirements of that section in deferring Warshak’s notice of the NuVox and Yahoo orders. See discussion and citations at note 15, *infra*.

<sup>14</sup> The United States further observes that 18 U.S.C. § 2712 provides for *only* monetary relief, and states that “[a]ny action against the United States under this subsection shall be the exclusive remedy against the United States for any claims within the purview of this section.” 18 U.S.C. § 2712(d); see also § 2708 (reiterating exclusivity of remedies); § 2707(b)(1) (providing injunctive relief for SCA violations by parties “other than the United States . . .”). It reasons that even if Warshak could show that the United States’ past 2703(d) orders violated the terms of the SCA, the Court could not rely on that showing to enjoin future 2703(d) orders. Because Warshak has established a sufficient likelihood of success on his Fourth Amendment claim, the Court need not decide, for purposes of the present Motion, whether the above-cited provisions would bar Warshak’s alternative claim for “injunctive relief against the United States for alleged *statutory* violations of the SCA.” (Doc. #15 at 5 (emphasis added); see also Part II.A.2, *supra*.)

interested parties, and (4) whether it would serve the public interest. Deja Vu, 274 F.3d at 400.

The Sixth Circuit has repeatedly recognized that “it is always in the public interest to prevent violation of a party’s constitutional rights.” Id. (citing G&V Lounge, Inc. v. Mich. Liquor Control Com’n., 23 F.3d 1071, 1079 (6<sup>th</sup> Cir. 1994)). Because the right to be free of unlawful government searches and seizures is a core concern of the Fourth Amendment, the fourth factor appears to weigh in favor of injunctive relief. The United States nonetheless asserts that both the third and fourth factors mitigate against relief because enjoining its use of 2703(d) would impede the public’s interest in both effective law enforcement and judicial deference to Congress’ judgment in crafting the SCA.<sup>15</sup> (Doc. #15 at 20.) Such considerations, however, cannot presumptively trump the grave constitutional concerns<sup>16</sup> presented by Warshak’s complaint and Motion. That is particularly true given that the specific injunctive relief contemplated by the Court should provide the United States an opportunity – when and if it elects to seek further 2703(d) orders against Warshak – to demonstrate why those orders should stand on less than a showing of probable cause. See discussion at Part II.B, infra.

The Court accordingly finds that all four factors weigh in favor of granting preliminary

---

<sup>15</sup> The United States observes that the SCA already provides that emails “in ‘electronic storage’ for less than 181 days” may only be seized “pursuant to a warrant based on probable cause,” and asserts that the Court should therefore defer to Congress’ reasoned judgment that the emails in question here are less deserving of protection. (Doc. #15 at 20; see also 18 U.S.C. § 2703(a).) While the Court need not reach the merits of this dispute for purposes of the present Order, it notes in passing Warshak’s contention that the United States misdefined “electronic storage” to seize emails of his, pursuant to 2703(d) orders, that – even under the SCA itself – should only have been seized pursuant to a warrant and on probable cause. (See, e.g., doc. #11 at 10-15.)

<sup>16</sup> The United States asserts that Warshak’s “claim that he is vindicating his constitutional rights is belied by the fact that it is unlikely that any of his constitutional rights are implicated by the facts alleged in his complaint.” (Doc. #15 at 20.) For the reasons set forth in its analysis of the first injunctive relief factor at Part II.A., supra, and at Part II.B, infra, the Court cannot agree.

injunctive relief to Warshak, and proceeds to determine the appropriate scope of that relief.

**B. Scope of Preliminary Injunction**

While the United States' past conduct in this case raises grave constitutional concerns, the Court is reluctant to conclude – absent some more concrete controversy – that any future seizure of Warshak's personal emails from a commercial ISP server pursuant to 18 U.S.C. 2703(d) would necessarily violate the Fourth Amendment. Plaintiffs' claims raise important questions – apparently of first impression in this Circuit – about the application of federal search and seizure law to electronic communications. As the United States observed at oral argument, the extent of Warshak's privacy expectations in a given email account – and hence the ultimate constitutionality of any warrantless seizure of emails stored in that account – could turn in part on facts specific to the account in question, such as the terms of the subscriber agreement between the ISP and Warshak.<sup>17</sup> As such, the Court finds that a broad injunction presumptively barring the United States from attempting to seize *any* of Warshak's emails by 18 U.S.C. § 2703(d) order is not warranted at this time.

It is clear, nonetheless, that a more tailored injunction is appropriate to minimize the risk that Warshak's Fourth Amendment rights will be infringed during the pendency of this litigation. As discussed above, the Court is not presently prepared to hold that 18 U.S.C. § 2703(d) facially violates the Fourth Amendment by simple virtue of the fact that it authorizes the seizure of personal emails from commercial ISPs without a warrant and on less than a showing of probable

---

<sup>17</sup> By way of example, the United States submitted that the terms of NuVox's subscriber agreement with Warshak differ from those of Yahoo's agreement and that the Yahoo terms were somewhat more expansive with respect to disclosure. The United States also contended, however, that the terms did not differ in any respect relevant to the Fourth Amendment inquiry of whether Warshak has a reasonable expectation of privacy in his emails.



cause. The constitutional concerns raised by 2703(d), however, do not end there. That is because 2703(d) – read in concert with the “delayed notice” exceptions at SCA subsections 2703(b)(1)(B)(ii) and 2705 – plainly authorizes the seizure of emails *not only* on less than a showing of probable cause and without a warrant, *but also* without notice to the subscriber. While the provisions do not purport to authorize *indefinite ex parte* seizures without some heightened showing of the necessity of secrecy, the facts of this case demonstrate how they have been applied to postpone notification for a year or more.<sup>18</sup>

The Court is provisionally persuaded that this combination of a standard of proof less than probable cause and potentially broad *ex parte* authorization cannot stand. The authorities cited at Part II.A.1 above suggest that at the very least, Warshak should have the opportunity to present his case – in the ripe, concrete context of a specific email account targeted but not yet seized by the United States – that 2703(d) orders issued on less than a showing of probable cause violate the Fourth Amendment. While this Court obviously cannot predict what the United States will do in the future, the United States’ past seizures of Warshak’s NuVox and Yahoo

---

<sup>18</sup> One complication, for purposes of this analysis, is that it is not entirely clear whether the United States and the Magistrate Judge adhered to the letter of the delayed-notice provisions in keeping Warshak’s NuVox and Yahoo orders under seal for a year and nine months, respectively. Section 2705 of the SCA, as incorporated by reference into 2703(b), provides that an order delaying notification may issue “for a period not to exceed ninety days.” 18 U.S.C. § 2705(a)(1)(A). The issuing court may then grant extensions of “up to ninety days each” if the United States establishes “that there is reason to believe that notification will result in (1) endangering the life or physical safety of an individual; (2) flight from prosecution; (3) destruction of or tampering with evidence; (4) intimidation of potential witnesses; or (5) otherwise seriously jeopardizing an investigation unduly delaying a trial.” There is no evidence of these periodic determinations in the docket for this case, or the Magistrate’s dockets for the NuVox and Yahoo seizures (obtained in hard copy by the Court). Rather, it appears that the Magistrate Judge simply ordered the orders and the United States’ applications for those orders “sealed until otherwise ordered by the Court,” and that they remained sealed for many multiples of ninety days until the United States moved, in late May 2006, for them to be unsealed. (See doc. #1 Ex. 1 at 2, Ex. 2 at 2 and docs. ##s 3-4 to 1:05-mj-135 and 1:05-mj-261.)

accounts and its refusal to commit not to undertake future seizures strongly suggest that, absent Court intervention, the United States may continue to invoke the SCA's *ex parte* provisions to deny Warshak that opportunity. To the extent that the United States wishes to avoid making a showing of probable cause and obtaining a warrant before undertaking future email seizures, it must at least notify Warshak of its intent to circumvent those standard constitutional protections.

To wit, the Court preliminary holds that 18 U.S.C. subsections §§ 2703(b)(1)(B)(ii), 2703(d) and 2705 violate the Fourth Amendment of the United States Constitution to the extent they collectively authorize the *ex parte* issuance of search and seizure orders without a warrant and on less than a showing of a probable cause. While the Court's ruling is predicated in part on its recognition of the threat of irreparable injury to Steven Warshak and other individuals whose emails have already been seized pursuant to such orders,<sup>19</sup> the constitutional flaws identified above are facial in nature. As such, the Court preliminarily **ENJOINS** the United States from moving to seize or seizing, pursuant to 18 U.S.C. § 2703(d), the contents of any personal email account maintained by an Internet Service Provider in the name of any resident of the Southern District of Ohio, including but not limited to Steve Warshak, without providing the relevant account holder or subscriber prior notice and an opportunity to be heard.

### **III. CONCLUSION**

For the reasons above, Plaintiff Steven Warshak's Motion for Temporary Restraining Order and/or Preliminary Injunction (doc. #11) is **GRANTED IN PART** and **DENIED IN**

---

<sup>19</sup> Intervenor-Plaintiff Harriet Warshak has submitted that the United States relied on an *ex parte* 2703(d) order virtually identical to the NuVox and Yahoo orders issued against Warshak to seize the contents of an email account maintained in her name by MSN Hotmail. (Doc. #13 at 1-2, 5-6, and Ex. C.)

**PART.** The United States is accordingly **ENJOINED**, pending final judgment on the merits of Plaintiffs' claims, from seizing, pursuant to court order under 18 U.S.C. § 2703(d), the contents of any personal email account maintained by an Internet Service Provider in the name of any resident of the Southern District of Ohio without providing the relevant account holder or subscriber prior notice and an opportunity to be heard on any complaint, motion, or other pleading seeking issuance of such an order.

IT IS SO ORDERED.

\_\_\_\_s/Susan J. Dlott\_\_\_\_\_  
Susan J. Dlott  
United States District Judge